UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

BAOLI YANG and
JIE YU,

Defendants.
_____/

INDICTMENT

The Grand Jury charges:

COUNT 1
(Wire Fraud)

Beginning on or about April 27, 2019 and continuing through on or about May 17, 2019, in Ingham County, in the Southern Division of the Western District of Michigan,

BAOLI YANG and
JIE YU

knowingly and unlawfully devised a scheme and artifice to defraud and to obtain money by means of false pretenses, representations and promises. Specifically, the defendants accessed the computer system of YANG's former employer without authorization, and demanded a pre-paid "employment contract" to stop interfering with its business operations.

BACKGROUND

1. In 2009, Baoli Yang ("YANG") was hired as an information technology ("IT") technician at Top Flite Financial ("TFF"), a mortgage servicing company in Williamston, Michigan. In that capacity, he serviced the company's internal computer systems, and had access to its network for security and maintenance purposes. TFF assigned YANG a unique employee

identification number, username and password ("credentials") to log into its network, and allowed him to work remotely from his home in Okemos, Michigan. YANG was not involved in the company's mortgage business or human resources department, and was not authorized to alter or delete financial account information or personnel files. TFF terminated YANG on or about April 27, 2019. At all times relevant to the indictment, Jie YU ("YU") was YANG's spouse, and resided with him in Okemos, Michigan. YU was not employed by TFF or assigned credentials to access its systems.

THE SCHEME AND ARTIFICE

2. After learning YANG had been terminated by TFF, the defendants continued to access TFF's internal network using YANG's credentials, and using the credentials of other TFF employees without their permission. The defendants accessed TFF's computer system on approximately 1,400 occasions after YANG's termination, and intentionally interfered with TFF's business operations by transferring funds between its internal accounts, deleting loan files, and altering payroll and personnel data.

3. The defendants also "booby trapped" TFF's computer system by adding unauthorized code to its login protocol before YANG's termination. The altered code instructed the system to search for YANG's credentials whenever a user logged in. If the system did not find YANG's credentials it would shut down, effectively halting TFF's business operations and foiling attempts to block the defendants' access to the system. YANG requested financial compensation, including a pre-paid three month contract worth $24,000, to "fix" the network problems the defendants had created.

WIRE COMMUNICATIONS

In furtherance of and for the purpose of executing the scheme described above, the defendants transmitted and caused to be transmitted in interstate commerce by means of wire communication certain signs and signals, including the following:

1. On or before April 29, 2019, using the internet, the defendants altered code in "neemsoft.dll" files that permitted authorized users to access TFF's system with a username and password.

2. On or about April 29, 2019, after the code he inserted caused TFF's computer system to shut down, YANG sent an e-mail to T.B., the Chief Executive Officer of TFF. YANG wrote, "I do not feel comfortable to log into the system and work on fixing anything unless we have a new contract." YANG demanded the new contract be "renewed quarterly, and the services fee should be prepaid three months ahead." In addition, YANG demanded TFF demote Senior IT Technician C.B., and deny C.B. access to the system except as authorized by YANG.

3. The defendants accessed TFF's network over the internet without authorization and caused the damage described below:

a. On or about May 8, 2019, the defendants used the C.B.'s credentials to disable the employee access of five TFF employees, including CEO T.B., preventing them from logging on to TFF's network.

b. On or about May 8, 2019, the defendants used the credentials of TFF Human Resources Manager T.F. to delete data relating to TFF loan number xxxxx4820.

c. On or about May 9, 2019, the defendants used C.B.'s credentials to transfer expense account funds from TFF Branch 285 (located outside the State of Michigan) to C.B.'s payroll account.

d. On or about May 10, 2019, the defendants used C.B.'s credentials to delete data relating to TFF loan number xxxxx3299.

e. On or about May 10, 2019, the defendants used C.B.'s credentials to delete data relating to TFF loan number xxxxx4856.

18 U.S.C. § 1343
18 U.S.C. § 2

COUNT 2
(Computer Intrusion Causing Damage)

Beginning on or about April 27, 2019 and continuing through on or about May 17, 2019, in Ingham County, in the Southern Division of the Western District of Michigan,

BAOLI YANG and
JIE YU

knowingly caused the transmission of computer programs, codes and commands, and as a result of such conduct, intentionally caused damage without authorization to a protected computer which was used in or affecting interstate or foreign commerce or communication, that is, the server of Top Flite Financial, with such damage causing loss to Top Flite Financial during the one year period beginning on or about May 17, 2018, aggregating at least $5,000 in value during such one year period.

18 U.S.C. § 1030(a)(5)(A)
18 U.S.C. § 1030(c)(4)(B)(i)
18 U.S.C. § 1030(e)(2)(B), (e)(8)

A TRUE BILL

_____
GRAND JURY FOREPERSON

ANDREW BYERLY BIRGE
United States Attorney

_____
NILS R. KESSLER
Assistant United States Attorney